AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Target Cell Phone, Target Facebook Accounts, & Target Google Accounts more particularly described in Attachments A1, A2 & A3

Case No. MJ18-584

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Target Cell Phone, Target Facebook Accounts, & Target Google Accounts more particularly described in Attachments A1, A2 & A3, attached hereto and incorporated herein.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachments B1, B2, & B3 hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 249	Hate Crimes
18 USC 2261A	Stalking
18 USC 371	Conspiracy

The application is based on these facts:
See affidavit which is attached hereto and incorporated herein by this reference.

- ☑ Continued on the attached sheet.
- ☑ Delayed notice of 30 days (give exact ending date if more than 30 days: 02/03/2019) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Ariana Kroshinsky, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 12/21/2018

Judge's signature

City and state: Seattle, Washington

Mary Alice Theiler, United States Magistrate Judge
Printed name and title

USAO #2018R01525

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, Ariana Kroshinsky, having been duly sworn, state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been since May 2018. I am presently assigned to a squad in the Seattle Field Office that covers civil rights crimes. My training and experience includes investigations of various federal criminal violations, including hate crimes and internet crimes. I have attended the Federal Bureau of Investigation Special Agent Training Course. I have participated in several hate crimes and internet crimes investigations, including conducting physical surveillance and executing search warrants.

II. PURPOSE OF AFFIDAVIT

3. I make this affidavit in support of an application for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), to acquire information associated with the following accounts that are stored at premises controlled by an electronic communications service and remote computer service provider, namely:

a. **T-Mobile Wireless**, a wireless telephone service provider headquartered at 3625 132nd Ave SE, Bellevue, WA 98006, for information about the historical location from October 20, 2018 through October 27, 2018, of the cellular telephone assigned call number 206-407-4936, hereinafter "**Target Cell Phone**" ;

b. **Facebook, Inc**. located at 1601 Willow Road, Menlo Park, California, to search the following accounts: UID: 1279801734; UID: 100023633720499; and UID: 100002532176517, hereafter "**Target Facebook Accounts**," and disclose to the government all content, call logs, and messages sent and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

received on the **Target Facebook Accounts**, as more fully described in Attachment A2.

c. **Google, Inc.,** located at 1600 Amphitheatre Parkway, Mountain View, California 94043, to search for and provide Google + Accounts: UID: 117906598794476810352, hereafter **Target Google Account** for any data, content, logs, log in, and any data backed up and stored from third party accounts on the **Target Google Account**.

4. More specifically, I am requesting warrants for the **Target Cellphone, Facebook,** and **Google Accounts**, in order to receive historical data and other records in order to ascertain the user's recent whereabouts when using the said accounts, which would assist the investigation in locating and securing evidence and instrumentalities related to criminal activity described and referenced herein and a criminal investigation occurring in this judicial district. Further, the subjects' location is relevant to his/her participation in some of the acts committed against the victim.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections: 249 (hate crimes), 2261A (stalking), and 371 (conspiracy), have been and are being committed by persons known and unknown including the user of the **Target Cellphone, Facebook,** and **Google Accounts**, namely, Marie Christine Fanyo-Patcho, Rodrigue Fodjo Kamden and Christian Fredy Djoko. There is also probable cause to search the information described in Attachments A1-3 for the items described in Attachments B1-3 to assist in obtaining possession of evidence, instrumentalities, contraband or fruits of these crimes.

6. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement personnel and computer scientists; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

information gained through my training and experience. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

III. JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction," as defined by 18 U.S.C. §§ 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), 2703(c)(1)(A), and 2711. Specifically, the Court is "a district court of the United States that – has jurisdiction over the offense[s] being investigated." 18 U.S.C. § 2711(3)(A)(i).

IV. SUMMARY OF PROBABLE CAUSE

8. The victim, U.M., and subjects of the investigation, Rodrigue Fodjo Kamden (hereafter "Kamden"), Christian Fredy Djoko (hereafter "Djoko"), and Marie Christine Fanyo-Patcho (hereafter "Fanyo-Patcho"), are all from Cameroon, a country located in West Africa. The official languages are French and English, though French is the primary language spoken. Christianity is the dominate faith. According to the U.S. Department of State's Cameroon 2017 Human Rights Report, in Cameroon homosexuality is illegal and can result in imprisonment from 6 months up to five years and fines of $37-373. Members of the LBGT community in Cameroon are often targeted for threats and harassment.

9. Between approximately September 2018, through November 2018, following a disagreement between U.M. and Fanyo-Patcho, the subjects began seeking to harass, embarrass, and humiliate U.M. by posting and texting personal and intimate content about U.M.'s sexual preference to other members of the Cameroon community as well as U.M.'s family members. The subjects used Facebook, WhatsApp, and Google + to post this information and communicate with one another and others.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

10. In approximately 2014, U.M. came to the United States on a student visa to attend school. Sometime after he arrived in the Seattle area, U.M. became involved in a relationship with another man and in approximately 2016, the two were married.

11. In approximately December 2017, Marie Christine Fanyo-Patchou (Fanyo-Patchou), a friend of U.M. from Cameroon, came to visit him and stayed in his apartment. According to U.M. while they were living in Cameroon and attending high school, he had disclosed to Fanyo-Patcho that he was gay. Before Fanyo-Patchou came to visit, U.M. had told her that he had gotten married to a man.

12. After Fanyo-Patchou began living with U.M., she constantly told him that being gay was not right and tried to convince him to be heterosexual. Fanyo-Patchou offered to help U.M. become heterosexual by having sexual intercourse with him. At one point Fanyo-Patchou asked him what he thought would happen if members of the Cameroon community learned he was gay and had a husband.

13. In late September 2018, U.M. told Fanyo-Patchou that she could no longer live in his residence. Fanyo-Patcho went to stay with another associate of hers, Rodrigue Fodjo Kamden (Kamden). Unbeknownst to U.M., when Fanyo-Patchou moved out, she took a cell phone that U.M. had given her to use. On the phone were intimate photographs of U.M. with his husband. Further, while living with U.M., she had secretly taken photos of U.M.'s personal photograph collection that documented his marriage. Some of the photographs that Fanyo-Patchou copied were private and contained nudity.

14. After moving in with Kamden, Fanyo-Patchou shared the photographs of U.M. and his husband with Kamden and another associate, Christian Fredy Djoko (Djoko). Shortly thereafter, Kamden and Djoko began releasing the photographs of U.M. and his husband online to members of Cameroon community via text message, the Google + platform of Whatsapp, and Facebook. After the photographs of U.M. were posted online, U.M. stated that he started receiving threatening texts and voicemail messages from unknown numbers with the Cameroonian country code.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

15. On October 22, 2018, U.M. called 911 to report that he had been assaulted. Seattle Police Officer, Joshua Brilla, responded. Officer Brilla met with U.M. who reported that on October 21, 2018, at approximately 1:00 A.M., he had parked his car and was walking toward his residence when he was approached by two Cameroonian men who called out to him in French using Cameroonian slang. U.M. has subsequently identified the men as Kamden and Djoko. U.M. stated that Djoko grabbed him from behind and pulled his wrists behind his back while Kamden grabbed his ears and pulled him to his knees. U.M. stated that the men were squeezing him and were calling him "faggot" and making other derogatory comments about his sexual orientation. U.M. also reported that the men said, "she tried to make you change but you didn't want to." U.M. interpreted this to mean that Fanyo-Patcho had tried to convert him to be heterosexual but he didn't convert.

16. After the assault ended U.M. returned to his residence. Later in the morning he called his brother and told him what happened. The following day he called a gay rights support service who urged him to report the attack to the police, which he did on Monday, October 22, 2018. Officer Brilla noted that U.M. suffered injuries/bruising to his ears and knees.

17. In subsequent interviews with law enforcement, U.M. has disclosed that the men were armed with a kitchen knife and that in addition to physically grabbing him, that Kamden forced his penis into U.M.'s mouth.

18. On October 25, 2018, U.M. reported to the Seattle Police that Fanyo-Patchou posted on her Facebook page in French that, "the faggot of Seattle needs to kill himself after writing his will" which U.M. interpreted as referring to him. Kamden responds "don't worry it's in the process. I already told you not to go that way. You will lose."

19. U.M. also received texts from mobile number (206) 407-4936 (**Target Cell Phone**) which he believed to be Kamden's mobile phone. One of the messages stated that U.M. needed to calm down or his "faggot husband photos would be posted online."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Another text from the **Target Cell Phone** referenced that U.M. should not have tried to serve him papers (U.M. had Kamden and Djoko both served with anti-harassment orders). U.M. said he also received three phone calls from the **Target Cell Phone** but he did not answer them (a search of the Accurint database showed (206) 407-4936 is a T-Mobile account belonging to Rodrigue Fodjo Kamden of Lynnwood, Washington). These phone calls violated the anti-harassment order.

20. U.M. has seen postings that Kamden and Djoko have posted on Facebook, to which they attached sexual photos of U.M., announcing that U.M. is gay and "prostituting" himself in America to make money. Multiple relatives of U.M. have told him that Kamden has texted them the photographs.

21. On November 2, 2018, U.M. reported that unknown persons spray-painted his vehicle with the words, "Dirty" and "Fag" and images in the shape of penises.

22. I learned that Kamden's Facebook user account identification is 1279801734 and that his Google+ account identification is 117906598794476810352.

23. I have learned that Djoko's Facebook account identification is 100023633720499, his Google + account information is 114036295919816718188.

24. Fanyo-Patchou's Facebook Account is 100002532176517.

25. Because Kamden and Djoko are both frequent users of text messaging and social media including Facebook, WhatsApp, and Google +, I believe that the geolocation data requested is relevant and material to the ongoing criminal investigation and will likely reveal fruits, contraband, instrumentalities, or evidence of violation of Title 18, United States Code, Sections of 249 (hate crimes), 370 (conspiracy) and 2261A (Stalking).

26. On November 3, 2018, Kamden and Djoko were arrested for the assault on U.M. Kamden's phone, (206) 407-4936 (**Target Cell Phone**) was taken from Kamden. On or about November 5, 2018, Kamden was released from custody when charges were not formally filed.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

27. Detective Tim DeVore of the Seattle Police Department obtained a search warrant to search the **Target Cell Phone.** I have reviewed the contents of the **Target Cell Phone**. In reviewing the photos and text messages copied from Kamden's phone by the Seattle Police Department, I learned that Kamden frequently used WhatsApp and had taken screenshots of some of his WhatsApp and text message conversations, including conversations with Cameroonian phone numbers to which he sent the pictures of U.M. Kamden had multiple copies of the pictures of U.M., including the photos taken by Fanyo-Patchou from U.M.'s hardcopy photo albums, photos in his tablet, and photos of his marriage certificate. There was a screenshot of a conversation between Kamden and "Marie de Seattle" (whom I believe to be Fanyo-Patchou) in which Fanyo-Patchou texted the photos of U.M. to Kamden. Also on Kamden's phone was a screenshot of a text message conversation that had taken place between U.M. and Djoko where U.M. revealed he was gay. There was a screenshot of a WhatsApp conversation between Kamden and U.M.'s father showing that Kamden sent him the photos, U.M.'s marriage certificate, and a photo of a sexual conversation U.M. had with another man on his tablet. There was a screenshot of a Facebook post Kamden had made describing U.M. as gay.

Target Cell Phone

28. In my training and experience, I have learned that T-Mobile is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone services have technical capabilities that allow them to collect and generate at least two kinds of information about the locations of the cellular telephones to which they provide service: (1) E-911 Phase II data, also known as GPS data or latitude-longitude data, and (2) cell-site data, also known as "tower/face information" or cell tower/sector records. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device's signal using data from several of the provider's cell towers. Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data is typically less precise than E-911 Phase II data.

29. Based on my training and experience, I know that providers of cell service such as T-Mobile can collect E-911 Phase II data about the location of the **Target Cell Phone**, including by initiating a signal to determine the location of the **Target Cell Phone** on the provider's network or with such other reference points as may be reasonably available.

30. Based on my training and experience, I know that providers such as T-Mobile can collect cell-site data about the **Target Cell Phone**.

31. In my training and experience, I have learned that cellular phones and other cellular devices communicate wirelessly across a network of cellular infrastructure, including towers that route and connect individual communications. When sending or receiving a communication, a cellular device broadcasts certain signals to the cellular tower that is routing its communication. These signals include a cellular device's unique identifiers.

32. I believe the collection of E-911 Phase II data and cell-site data related to the **Target Cell Phone** has relevant information related to the crimes against U.M. Specifically, it will show the location of the **Target Cell Phone** on the date that U.M. was assaulted.

Facebook Technical Background

33. Facebook, Inc. (hereafter Facebook) owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts through which users can share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

34. Facebook asks users to provide basic contact information, either during the registration process or thereafter. This information may include the user's full name, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

35. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information in the user's account available only to himself or herself, to other specified Facebook users, to all Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook. Depending on the user's privacy settings, Facebook may also obtain and store the physical location of the user's device(s) as they interact with the Facebook service on those device(s).

36. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "Mini-Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

37. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. A particular user's profile page also includes a "Wall," which is a

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

38. Facebook has a Photos application, where users can upload an unlimited number of albums and photos. Another feature of the Photos application is the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, a user's "Photoprint" includes all photos uploaded by that user that have not been deleted, as well as all photos uploaded by any user that have that user tagged in them.

39. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile.

40. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

41. The Facebook Gifts feature allows users to send virtual "gifts" to their friends that appear as icons on the recipient's profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other "pokes," which are free and simply result in a notification to the recipient that he or she has been "poked" by the sender.

42. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

43. Some Facebook pages are affiliated with groups of users, rather than one individual user. Membership in the group is monitored and regulated by the administrator or head of the group, who can invite new members and reject or accept requests by users to enter. Facebook can identify all users who are currently registered to a particular group and can identify the administrator and creator of the group. Facebook also assigns a group identification number to each group. Facebook uses the term "Group Contact Info" to describe the contact information for the group's creator and administrator, as well as the current status of the group profile page.

44. Facebook uses the term "Neoprint" to describe an expanded view of a given user profile. The "Neoprint" for a given user can include the following information from the user's profile: profile contact information; Mini-Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

45. Facebook also retains IP address logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action.

46. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service used, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

support services, as well records of any actions taken by the provider or user as a result of the communications.

47. Therefore, the computers of Facebook are likely to contain all the material just described, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and account application.

Background Regarding Google's Services

48. In my training and experience, I have learned that Google provides a wide variety of on-line services, including electronic mail ("e-mail") access and instant messaging (otherwise known as "chat" messaging), to the general public.

49. In addition to e-mail and chat, Google offers subscribers numerous other services including: Android, Blogger, Google Alerts, Google Calendar, Google Chrome Sync, Google Cloud Print, G-Suite, Google Developers Console, Google Drive, Google Hangouts, Google Maps, Google Payments, Google Photos, Google Search Console, Google Voice, Google+, Google Profile, Location History, Web & Activity, and YouTube, among others. Thus, a subscriber to a Google account can also store files, including address books, contact lists, calendar data, photographs and other files, on servers maintained and/or owned by Google. For example, Google Calendar is a calendar service that users may utilize to organize their schedule and share events with others. Google Drive may be used to store data and documents, including spreadsheets, written documents (such as Word or Word Perfect) and other documents that could be used to manage a website. Google Photos can be used to create photo albums, store photographs, and share photographs with others and "You Tube," allows users to view, store and share videos. Google Search Console records a Google account user's search queries. And Google Web & Activity records certain browsing history depending on whether the account holder is logged into their account. Google + is a Google social networking platform similar to Facebook. This platform provides Google users the ability to establish accounts through which users can share written news, photographs,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

videos, and other information with other Facebook users, and sometimes with the general public.[1] Records and data associated with third party-apps may also be stored on Google; for example, the app WhatsApp, an instant messaging service owned by Facebook, can be configured to back up a user's instant messaging to a Google user's account.

50. Like many internet service companies, the services Google offers are constantly changing and evolving.

51. Google also offers a suite of cloud computing services that runs on the same infrastructure that Google uses internally for its end-user products, such as Google Search and YouTube. Alongside a set of management tools, it provides a series of modular cloud services including computing, data storage, data analytics and machine learning to customers.

52. Based upon my training and experience, all of these types of information may be evidence of crimes under investigation. Stored e-mails and chats not only may contain communications relating to crimes, but also help identify the participants in those crimes. For example, address books and contact lists may help identify and locate co-conspirators. Similarly, photographs and videos of co-conspirators may help identify their true identities, as opposed to supposed identities that they have used in telephone or e-mail communications. Documents (such as Google sheets used to communicate with victim computers), may identify the scope of the criminal activity. And calendar data may reveal the timing and extent of criminal activity. Search and browsing history can also be extremely useful in identifying those using anonymous online accounts and may also constitute direct evidence of the crimes under investigation to the extent the browsing history or search history might include searches and browsing history related to computer intrusions, point of sale systems, victims, trafficking in stolen data and other evidence of the crimes under investigation or indications of the true identity of the account users.

---

[1] In October 2018, Google announced it would discontinue the service in approximately August 2019.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

A. Subscriber Records and Account Content

53. Subscribers obtain an account by registering with Google. When doing so, e-mail providers like Google ask the subscriber to provide certain personal identifying information. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users, and to help establish who has dominion and control over the account.

54. Google will retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's websites), and other log files that reflect usage of the account. In addition, Google will often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

55. In some cases, Google account users will communicate directly with the provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Google will typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation, because the information can be used to identify the account's user or users.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

56. Google is also able to provide information that will assist law enforcement in identifying other accounts associated with the **Target Google Accounts**, namely, information identifying and relating to other accounts used by the same subscriber. This information includes any forwarding or fetching accounts[2] relating to the **Target Google Accounts**, all other Google accounts linked to the **Target Google Accounts** because they were accessed from the same computer (referred to as "cookie overlap"), all other Google accounts that list the same SMS phone number as the **Target Google Accounts**, all other Google accounts that list the same recovery e-mail address[3] as do the **Target Google Accounts**, and all other Google accounts that share the same creation IP address as the **Target Google Accounts**. Information associated with these associated accounts will assist law enforcement in determining who controls the **Target Google Accounts** and will also help to identify other e-mail accounts and individuals relevant to the investigation.

Google Location History and Location Reporting

57. According to Google's website, "Location Reporting" allows Google to periodically store and use a device's most recent location data in connection with the Google Account connected to the device. "Location History" allows Google to store a history of location data from all devices where a user is logged into their Google Account and have enabled Location Reporting. According to Google "when you turn on Location Reporting for a device like your iPhone or iPad, it lets Google periodically store and use that device's most recent location data in connection with your Google Account." How often Location Reporting updates location data is not fixed. Frequency is determined by factors such as how much battery life the device has, if the device is moving, or how fast

---

[2] A forwarding or fetching account related to the **Target Google Accounts** would be a separate e-mail account that can be setup by the user to receive copies of all of the e-mail sent to the **Target Google Accounts**.

[3] The recovery e-mail address is an additional e-mail address supplied by the user that is used by Google to confirm your username after you create an e-mail account, help you if you are having trouble signing into your Google account or have forgotten your password, or alert you to any unusual activity involving user's Google e-mail address.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the device is moving. Google's location services may use GPS, Wi-Fi hotspots, and cellular network towers to determine an account holder's location.

58. Based on the above, I know that if a user of the **Target Google Accounts** utilizes a mobile device to access the respective account identified in Attachment A3 and has not disabled location services on his or her device/s or through the Google account settings, Google may have detailed records of the locations at which the account holders utilized the mobile device/s. This type of evidence may further assist in identifying the account holders, and lead to the discovery of other evidence of the crimes under investigation.

59. I know that Google's Android service collects and stores identifying information about an Android smart phone used to access the Google account, including the International Mobile Equipment Identifier (IMEI), International Mobile Subscriber Identity (IMSI), telephone number and mobile carrier code. I know that Google's Location History service periodically queries the physical location of a device that is currently accessing a Google account through the device's GPS, nearby Wi-Fi network IDs and cellular tower information and records a history of device movements in Google's servers. Because the criminal actors behind this malware scheme have made a concerted effort to disguise their real location, I am requesting Google to provide information from the Android service and Location History service from the **Target Google Accounts** in order to more accurately identify the location and phone number of the person responsible for the **Target Google Accounts**.

Information To Be Searched And Things To Be Seized

60. Pursuant to Title 18, United States Code, Section 2703(g), this application and affidavit for search warrants seeks authorization to permit T-Mobile Wireless, Facebook, Inc., and Google, Inc., and its agents and employees, to assist agents in the execution of this warrant. Once issued, the search warrants will be presented to T-Mobile Wireless, Facebook, Inc., and Google, Inc. with direction that each entity identify the account described in Attachments A1-3 to this affidavit, respectively, as well as other

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

subscriber and log records associated with each of the accounts, as set forth in Section I of Attachments B1-3 to this affidavit.

61. The search warrant will direct T-Mobile Wireless, Facebook, Inc., and Google, Inc. to create an exact copy of the specified account and records, including an exact copy of the contents of the hard disk drive or drives installed on the server associated with the **Target Accounts**, or the original drives.

62. I, and/or other law enforcement personnel will thereafter review the copy of the electronically stored data, and identify from among that content those items that come within the items identified in Section II to Attachment B, for seizure.

63. Analyzing the data contained in the forensic image may require special technical skills, equipment, and software. It could also be very time-consuming. Searching by keywords, for example, can yield thousands of "hits," each of which must then be reviewed in context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. Keywords used originally need to be modified continuously, based on interim results. Certain file formats, moreover, do not lend themselves to keyword searches, as keywords, search text, and many common e-mail, database and spreadsheet applications do not store data as searchable text. The data may be saved, instead, in proprietary non-text format. And, as the volume of storage allotted by service providers increases, the time it takes to properly analyze recovered data increases, as well. Consistent with the foregoing, searching the recovered data for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months. All forensic analysis of the data will employ only those search protocols and methodologies reasonably designed to identify and seize the items identified in Section II of Attachment B to the warrant.

V. REQUEST FOR DELAYING NOTICE

64. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

delay notice until 30 days after the collection authorized by the warrant has been completed. This delay is justified because there is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Based upon my knowledge, training, and experience, it is my belief that providing immediate notice to subscriber or user of the **Target Cell Phone, Facebook, and Google Accounts** may result in premature notification to Kamden, or the subscriber, of the existence of the authorization for telephone location tracking would alert them to the ongoing investigation, and this disclosure would jeopardize the continuation and efficacy of the investigation. Furthermore, premature notification to Kamden or the subscriber of the existence of the authorization for telephone location tracking prior to completion of the investigation would provide Kamden or the subscriber the opportunity to destroy evidence and flee the jurisdiction. *See* 18 U.S.C. § 3103a(b)(1). As further specified in Attachment B, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

VI. REQUEST FOR SEALING

65. I further request this Court issue an order sealing, until further order of the Court, all papers submitted in support of the requested search warrant, including the application, this affidavit, the attachments, and the requested search warrant. I believe sealing these documents is necessary because the information to be seized is relevant to an ongoing investigation, and any disclosure of the information at this time may cause Kamden, Djoko, Fanyo-Patcho, or others associated with **Target Cell Phone, Facebook, and Google Accounts**, to flee from prosecution, cause destruction of or tampering with evidence, or otherwise seriously jeopardize this investigation. Premature disclosure of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the contents of the application, this affidavit, the attachments, and the requested search warrant may adversely affect the integrity of the investigation.

VII. CONCLUSION

66. Based on the foregoing, I request that the Court issue the proposed search warrants, pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c). I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the **Target Cell Phone, Facebook, and Google Accounts** outside of daytime hours. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Accordingly, by this Affidavit and warrant I seek authority for the government to search all of the items specified in Section I of Attachment B1-3 (attached hereto and incorporated by reference herein) to the warrant, and specifically to seize all of the data, documents and records that are identified in Section II to that same Attachment.

67. I further request that the Court direct Provider to disclose to the government any information described in Attachment B that is within the possession, custody, or control of Provider. I also request that the Court direct Provider to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B unobtrusively and with a minimum of interference with Provider's services, including by initiating a signal to determine the location of the **Target Cell Phone, Facebook, and Google Accounts** on Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government.

//

//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

I declare under the penalty of perjury that the statements above are true and correct to the best of my knowledge and belief.

DATED this 21st day of December 2018.

ARIANA KROSHINSKY
Special Agent
Federal Bureau of Investigations

SUBSCRIBED AND SWORN before me this on this 21st day of December, 2018.

MARY ALICE THEILER
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-1

Target Cell Phone

1. This warrant applies to information associated with the cellular telephone assigned call number **206-407-4936**, with an International Mobile Subscriber Identifier("IMSI") number or Electronic Serial Number ("ESN") 353322/09/047605/3 (hereinafter "**Target Cell Phone**"), that is stormed at the premises owned, maintained, controlled, and/or operated T-Mobile Wireless, a wireless telephone service provider headquartered at 3625 132nd Ave SE, Bellevue, WA 98006.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B-1

T-Mobile - Particular Things to be Seized

A. The following information about the customers or subscribers of the Account(s):

1. Names (including subscriber names, user names, and screen names);

2. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);

3. Local and long distance telephone connection records;

4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;

5. Length of service (including start date) and types of service utilized;

6. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI"));

7. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and

8. Means and source of payment for such service (including any credit card or bank account numbers) and billing records.

B. All records and other information (not including the contents of communications) relating to the Account, including:

9. Records of user activity for each connection made to or from the Account(s), including log files; messaging logs; the date time, length, and method of connections, data transfer volume; user names; and source and destination Internet Protocol Addresses; cookie IDs; browser type;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

10. Information about each communication sent or received by the Account(s), including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers), and;

11. All information about the location of the Target Cell Phone described in Attachment A1 from October 20, 2018 through November 3, 2018, during all times of day and night, and the status of the device and the account associated with the device (i.e., whether the device is active or operational and whether the account is in good standing, canceled, suspended, etc.). "Information about the location of the Target Cell Phone" includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information, as well as all data about which "cell towers" (i.e., antenna towers covering specific geographic areas) and "sectors" (i.e., faces of the towers) received a radio signal from the cellular telephone described in Attachment A1.

12. To the extent that the information described in the previous paragraph (hereinafter, "Location Information") is within the possession, custody, or control of (wireless provider) (hereinafter "Provider"), Provider is required to disclose the Location Information to the government. In addition, Provider must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with Provider's services, including by initiating a signal to determine the location of the Target Cell Phone on Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate Provider for reasonable expenses incurred in furnishing such facilities or assistance.

13. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds it reasonable necessity for the seizure of the Location Information. See 18 U.S.C § 3103a(b)(2).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-2

Target Accounts Facebook, Inc.

1. This warrant applies to information associated with Facebook user IDs:

   a. 1279801734;

   b. 100023633720499; and

   c. 100002532176517

that are stored at the premises owned, maintained, controlled, or operated by Facebook, Inc. located at 1601 Willow Road, Menlo Park, California.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B -2

Facebook - Particular Things to be Seized

I. Information to be disclosed by Facebook

To the extent that the information for the account described in Attachment A-2, is within the possession, custody, or control of Facebook, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A-2:

(a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities;

(c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;

(d) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

(e) All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;

(f) All "check ins" and other location information;

(g) All IP logs, including all records of the IP addresses that logged into the account;

(h) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

(i) All information about the Facebook pages that the account is or was a "fan" of;

(j) All past and present lists of friends created by the account;

(k) All records of Facebook searches performed by the account;

(l) All information about the user's access and use of Facebook Marketplace;

(m) The types of service utilized by the user;

(n) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(o) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

(p) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within **14 days** of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that relates to the ongoing investigation of violations of 18 U.S.C. § § 241 and 249 (Conspiracy to Violate Civil Rights and Hate Crimes); and 18 U.S.C. § 2261A (Cyberstalking) involving Rodrigue Fodjo Kamden, Christian Fredy Djoko, and Marie Christine Fanyo-Patcho, including, for each user ID identified on Attachment A-2, information pertaining to the following matters:

(a) Any content including e-mails, messages, texts, photographs, visual images, documents, spreadsheets, address lists, contact lists or communications of any type which could be used to identify the user and or their location;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

(b) Records relating to who created, used, or communicated with the user ID, including records about their identities and whereabouts;

(c) All subscriber records associated with the specified accounts, including name, address, local and long distance telephone connection records, or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service including any credit card or bank account number;

(d) Any and all other log records, including IP address captures, associated with the specified accounts; and

(e) Any records of communications between Facebook and any person about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This is to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-3

Target Accounts Google, Inc.

1. This warrant applies to information associated with Google user identification numbers and Google + user id #'s:

   a. 117906598794476810352; and

   b. 114036295919816718188

that are stored at the premises owned, maintained, controlled, or operated by Google, Inc., located at 1600 Amphitheatre Parkway, Mountain View, California 94043.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B-3

Google - Particular Things to be Seized

Section I - Information to be disclosed by Google, for search:

To the extent that the information described in Attachment A-3 is within the possession, custody, or control of Google, including any e-mails, records, files, logs, backup data from third party apps such as WhatsApp, or information that has been deleted but is still available to Google or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the government for each account or identifier listed in Attachment A-3:

a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Section II - Information to be seized by the government

All information described above in Section I that constitutes evidence and instrumentalities of violations of 18 U.S.C. §§ 241 and 249 (conspiracy to violate civil rights or hate crimes); 18 U.S.C. §§ 2261A (Cyberstalking), involving Rodrigue Fodjo Kamden, Christian Fredy Djoko, and Marie Christine Fanyo-Patcho, for each account or identifier listed on Attachment A-3, information pertaining to the following matters:

a. The cyberstalking and harassment of U.M.;

b. All messages, documents, and profile information, attachments, or other data that serves to identify any persons who use or access the account specified, or who exercise in any way any dominion or control over the specified account;

c. Any address lists or buddy/contact lists associated with the specified account;

d. All subscriber records associated with the specified account, including name, address, local and long distance telephone connection records, or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account number;

e. Any and all other log records, including IP address captures, associated with the specified account;

f. Any records of communications between Google, and any person about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970